CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 106 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 10 mai 2018

Président

M. Bob Zimmer

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le jeudi 10 mai 2018

● (0845)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Je déclare ouverte la séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément à l'article 108(3)h)(vii) du Règlement, nous étudierons l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook.

Ce matin, la séance se déroulera en deux segments d'une heure. Nous entendrons le témoignage de la commissaire à l'information du Royaume-Uni, Mme Denham, par téléconférence. Nous accueillerons également M. McEvoy, du Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique.

Nous allons commencer par Mme Denham.

Mme Elizabeth Denham (commissaire à l'information, Bureau de la commissaire à l'information du Royaume-Uni): Je vous souhaite le bonjour depuis Manchester.

Je vous remercie, monsieur le président, ainsi que les membres du Comité, de m'avoir invitée à témoigner devant vous aujourd'hui.

Je suis commissaire à l'information du Royaume-Uni et, à ce titre, j'ai à réglementer la protection des données et l'accès à l'information et à appliquer une foule d'autres lois relatives aux renseignements personnels.

Je suis heureuse d'avoir l'occasion de vous parler aujourd'hui du travail accompli par mon bureau dans son enquête sur l'utilisation des données personnelles à des fins de campagne politique.

Ayant suivi avec beaucoup d'intérêt certaines des séances précédentes du Comité portant sur cette étude, je pense devoir, d'entrée de jeu, apporter quelques précisions.

Au Royaume-Uni, comme dans l'ensemble de l'Union européenne, l'information sur les opinions politiques des particuliers est considérée comme une catégorie de données personnelles particulièrement sensibles à laquelle des mesures de protection supplémentaires s'appliquent en vertu des lois sur la protection des données. Cela signifie donc que les partis et les campagnes politiques sont régis par un ensemble de mesures légales visant la protection des données, le marketing direct et les élections lorsqu'ils traitent des données à des fins électorales, le tout sous la surveillance de mon bureau et de la commission électorale. Cela a toujours été le cas depuis l'adoption de la loi sur la protection des données il y a plus de 20 ans, et c'est simplement admis comme une norme culturelle.

Ces règles sont en place pour assurer la tenue d'élections libres et justes et elles n'entravent pas l'engagement démocratique au Royaume-Uni, mais obligent plutôt les partis politiques à communiquer avec les électeurs d'une manière qui y soit conforme. Vu la place spéciale des partis politiques dans une société démocratique, ils ont obtenu un statut particulier aux termes de la loi britannique sur la protection des données qui leur permet de mener leurs activités de campagne.

Dans mon rôle de traitement des plaintes, j'examine les plaintes formulées à l'endroit des partis politiques par les particuliers qui pensent que leurs données ont été utilisées à mauvais escient. Le nombre de plaintes n'a jamais été particulièrement élevé. Mis à part un pic au moment des élections, les partis politiques n'ont pas été, dans l'ensemble, à l'origine d'une forte proportion des plaintes. Mon bureau a maintenu un dialogue continu avec les partis, les a rencontrés régulièrement et leur a donné des directives sur la façon de se conformer à la loi lorsqu'ils font campagne.

Toutefois, le référendum de juin 2016 sur l'appartenance du Royaume-Uni à l'Union européenne en a été un événement inhabituel dans la vie politique britannique. Au lieu d'être dirigée par les partis politiques établis, la campagne référendaire a été menée par des groupes de campagne qui étaient, dans certains cas, des coalitions floues d'organismes aux vues similaires. La loi du Royaume-Uni sur la protection des données est libellée de façon à cibler les partis politiques, mais, dans ce pays où les référendums sont rares, elle est quelque peu laconique au sujet des groupes de campagne non partisans. Compte tenu des possibilités d'infraction à la loi pendant la campagne référendaire, la tâche de mon bureau devenait plus difficile.

Nous étions préoccupés par certaines des pratiques de campagne dont nous entendions parler et par la provenance des données personnelles utilisées par les groupes de campagne pour cibler les votants. C'est pourquoi, en mai 2017, j'ai annoncé une enquête officielle sur le recours à l'analytique des données à des fins politiques. À l'origine, l'enquête visait à lever le voile sur la façon dont les renseignements personnels étaient utilisés dans les campagnes politiques modernes.

Au départ, la loi sur la protection des données exige que les organisations traitent les données de façon équitable et transparente, mais la rapidité des développements sociaux et technologiques dans l'utilisation des mégadonnées a eu pour effet que les connaissances ou la transparence font défaut quant aux techniques de traitement des données, y compris l'analyse, les algorithmes, le couplage de données et le profilage à des fins de microciblage des consommateurs et des électeurs.

Je pense que ces techniques sont attrayantes pour les partis politiques en campagne, car elles leur permettent de cibler des électeurs individuels au moyen de messages qui correspondent à leurs intérêts et à leurs valeurs politiques, mais il ne s'agit pas simplement d'un nouveau jeu joué selon des règles différentes. La loi continue de s'appliquer, que la campagne se déroule hors ligne ou en ligne.

● (0850)

Mon enquête porte maintenant sur plus de 30 organismes, y compris des partis politiques et des campagnes, des sociétés de données et des plateformes de médias sociaux. Parmi ces organisations, il y a AggregateIQ, qui a été utilisée par un certain nombre de groupes de campagne au Royaume-Uni, une entreprise dont le Comité a déjà entendu parler.

Ce à quoi nous ne nous attendions pas au début de notre enquête, c'était d'avoir à déterminer quoi, quand, comment, pourquoi et par qui avaient été utilisées les données provenant d'un total de 87 millions de profils Facebook, extraites par un universitaire et transmises à un consultant politique du Royaume-Uni travaillant à l'élection de 2016 aux États-Unis et à d'autres campagnes politiques. Nous avons dû nous pencher aussi sur plusieurs autres sujets d'enquête dont je ne peux pas parler pour l'instant. Cela a naturellement soulevé des préoccupations au Royaume-Uni et à l'étranger, et des agents de Facebook et de Cambridge Analytica ont été appelés à rendre des comptes dans divers parlements nationaux.

Je suis sûre que vous comprenez que je ne peux pas parler des détails d'une enquête en cours. L'enquête progresse à un rythme soutenu. Les activités d'application de la loi sont en cours, et il ne serait donc pas approprié que je fasse d'autres commentaires.

Ce que je peux dire, cependant, c'est qu'un certain nombre d'organismes ont coopéré librement à notre enquête. Ils ont répondu à nos questions et nous ont consultés. Mais d'autres ont tenté de miner l'enquête en ne fournissant pas de réponses complètes à nos questions, en refusant de collaborer ou en contestant le processus. Dans ces situations, nous avons été obligés d'exercer nos pouvoirs légaux pour faire des demandes officielles d'information.

Certains de mes champs d'enquête sont plus avancés que d'autres, mais un rapport à jour de toute l'enquête sera publié par mon bureau au cours des prochaines semaines. Pendant que mon collègue, le commissaire Therrien, mène sa propre enquête sur Facebook, il y a des domaines d'intérêt commun qui recoupent nos deux enquêtes. Comme le commissaire Therrien l'a fait remarquer, le Bureau de la commissaire à l'information et le Commissariat à la protection de la vie privée entretiennent une relation de collaboration et nous pouvons échanger des renseignements si cela est nécessaire à nos fins d'enquête dans l'intérêt public.

Lorsque je pense aux travaux de votre comité, je vois deux champs d'enquête distincts, d'abord, le problème immédiat de Facebook, AggregateIQ et d'autres et la possibilité d'infractions aux lois canadiennes, puis une deuxième ligne d'enquête à plus long terme, portant sur la question plus vaste des attentes du public à l'égard de l'utilisation de leurs données dans le contexte politique et de la nécessité éventuelle de modifier la loi. Cette enquête porte, à juste titre, non seulement sur la loi sur la protection des données, mais aussi sur d'autres domaines, comme la loi électorale, pour voir comment ces problèmes peuvent être réglés.

J'ai mentionné que mon rapport serait publié au cours des prochaines semaines. Je vais déterminer si les droits des particuliers ont été violés, mais je vais aussi formuler des recommandations sur la façon dont le gouvernement, au Royaume-Uni et dans d'autres pays, pourrait remédier aux lacunes que j'ai constatées, y compris le besoin d'une plus grande transparence dans les campagnes politiques. Bien que chaque pays soit différent, il y a peut-être des leçons pertinentes qui pourraient s'appliquer au contexte canadien.

Pour mettre mes cartes sur la table, et je dis cela dans le contexte en reconnaissant pleinement l'intérêt public que revêt la capacité pour les partis politiques de pouvoir communiquer avec les électeurs, ce qui est bien sûr une pierre angulaire de l'engagement démocratique, je crois que l'utilisation des données personnelles par les partis politiques doit être traitée dans la loi canadienne. Les Canadiens devraient pouvoir déposer une plainte auprès d'un organisme de réglementation indépendant.

La loi que nous avons au Royaume-Uni est fondée sur des principes et des bases solides et n'entrave pas inutilement le processus démocratique. Dans la loi sur la protection des données du Royaume-Uni, les partis politiques ont une justification juridique pour traiter les données personnelles des personnes lorsqu'elles sont utilisées à des fins électorales.

● (0855)

Mon bureau n'est qu'un des organismes de surveillance au Royaume-Uni. La commission électorale du Royaume-Uni est chargée de superviser les élections et les dépenses politiques. Lorsqu'il y a des recoupements, mon bureau peut travailler avec la commission électorale ou décider quel organisme devrait avoir l'initiative.

Cela ne veut pas dire que le régime de protection des données du Royaume-Uni est parfait. J'ai dit que, à tout prendre, le système fonctionne bien lorsqu'il s'agit des partis politiques. Le référendum sur le Brexit était autre chose, comme je l'ai dit plus tôt. Des groupes de campagne non traditionnels, qui ne connaissent pas la loi sur la protection des données ou qui ne s'en soucient pas, sont peut-être tombés dans l'illégalité, et je pense que le caractère provisoire de ces groupes a rendu plus difficiles les poursuites judiciaires contre eux pour avoir enfreint la loi sur la protection des données.

La loi du Royaume-Uni me donne déjà le droit de recourir à des sanctions pénales si un avis de mon bureau demeure sans réponse. Cela veut dire que même si un groupe de campagne ou un organisme se dissout, je peux toujours poursuivre leurs ex-dirigeants. Ce pouvoir peut sembler exorbitant, mais, en tant qu'organisme de réglementation, je dois rendre des comptes au Parlement et je dois être en mesure de justifier la façon dont j'applique mes pouvoirs de réglementation. Je pense que le Bureau de la commissaire à l'information a toujours été un organisme qui exerçait ses pouvoirs de réglementation de manière proportionnée et responsable, et jamais plus que dans le contexte d'une campagne politique où nous sommes très conscients de l'intérêt public inhérent à l'engagement démocratique. Cette approche sera maintenue pour l'application du RGPD et, après son adoption, pour la future loi sur la protection des données du Royaume-Uni.

La manipulation des électeurs par le microciblage risque de miner notre modèle démocratique. N'est-ce pas une préoccupation majeure pour nous tous?

Merci beaucoup de votre attention. Je serai heureux de répondre à vos questions.

● (0900)

Le président: Merci, madame Denham.

Nous allons passer à M. McEvoy.

Allez-y.

M. Michael McEvoy (commissaire, Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique): Bonjour, monsieur le président, et merci beaucoup au Comité de m'avoir invité à comparaître ce matin, en particulier en compagnie — c'est un grand plaisir — de ma collègue commissaire Denham du Royaume-Uni. En fait, il y a à peine quelques semaines, j'étais au Royaume-Uni pour aider la commissaire Denham à mener l'enquête dont elle a parlé.

Peu de temps après mon retour en Colombie-Britannique, je discutais avec le commissaire Therrien du Commissariat à la protection de la vie privée du Canada pour convenir de mener conjointement une enquête sur Facebook et AggregateIQ, société de la Colombie-Britannique que le Comité connaît très bien. L'enquête se poursuit. Bien entendu, je ne suis pas libre de divulguer grand-chose à ce sujet tant que notre travail ne sera pas achevé.

Ce que j'aimerais faire ce matin, c'est revenir sur les thèmes mentionnés par la commissaire Denham et qui concernent les aspects généraux du mandat de votre comité. Je parle de la recherche de solutions législatives qui aideront à garantir aux Canadiens la confidentialité de leurs données et l'intégrité de nos processus démocratiques et électoraux.

Au-delà de nos enquêtes sur des sociétés comme Facebook et Cambridge Analytica, qui sont des enquêtes cruciales, il est important que les partis politiques du Canada eux-mêmes prennent des mesures pour rétablir la confiance dans les processus démocratiques de notre pays. Je vous invite, comme mon collègue, le commissaire Therrien, à vous soumettre à des mesures de reddition de comptes concernant la façon dont vous recueillez et utilisez l'information des électeurs canadiens.

Une question qui mérite réflexion, à mon avis, est celle de savoir si le scandale de Cambridge Analytica se serait produit n'eurent été les pressions croissantes exercées sur les partis politiques pour qu'ils recueillent et analysent des données personnelles dans l'espoir de les comprendre et de les utiliser pour persuader les électeurs. La démocratie exige que les citoyens aient confiance dans le processus politique, et un élément important de ce processus concerne la façon dont les partis politiques recueillent et utilisent les renseignements personnels qui appartiennent aux Canadiens.

Le Parlement et certaines assemblées législatives provinciales ont créé des bureaux qui surveillent la collecte et l'utilisation des renseignements personnels par des organismes privés et publics. Curieusement, cette surveillance, à quelques exceptions près, ne s'applique pas aux partis politiques. La Colombie-Britannique est une exception. La Personal Information Protection Act de la Colombie-Britannique, ou PIPA, s'applique à tous les organismes de la Colombie-Britannique. Elle est, pour l'essentiel, semblable à la Loi sur la protection des renseignements personnels et les documents électroniques et, pour cette raison, elle prime généralement la LPRPDE dans ma province.

Les partis politiques de ma province sont assujettis à la PIPA depuis son adoption en 2004. Au cours des 14 années écoulées depuis son adoption, je peux vous assurer que la démocratie a continué de prospérer sans entrave en Colombie-Britannique. Nous n'avons été informés d'aucune préoccupation ou suggestion laissant entendre que les lois protégeant les renseignements personnels des électeurs limitent la capacité des partis politiques ou des candidats d'atteindre les électeurs.

Les partis politiques de la Colombie-Britannique peuvent recueillir des renseignements personnels sur les électeurs, et ils le font, mais en ayant les mêmes responsabilités et obligations juridiques raisonnables qui s'appliquent aux autres organismes.

En règle générale, cela signifie que les partis politiques obtiennent des renseignements avec le consentement des électeurs, accompagnés d'une explication claire de la façon dont ces renseignements seront utilisés et de la raison pour laquelle ils le seront. J'ai utilisé les mots « en règle générale » et « avec le consentement » parce qu'il y a des dispositions légales qui permettent aux partis de recueillir des renseignements sans consentement, particulièrement pour obtenir la liste électorale et d'autres données sur les électeurs d'Elections BC. Toutefois, ces dispositions sont assorties d'une condition selon laquelle le parti qui reçoit l'information doit fournir au directeur général des élections une politique satisfaisante en matière de protection de la vie privée.

La PIPA donne également aux citoyens le droit légal de connaître et de corriger les renseignements personnels que les partis politiques recueillent auprès d'eux et de déposer une plainte au besoin. Ces plaintes sont traitées par mon bureau. Le droit des citoyens d'exercer un contrôle sur leurs renseignements personnels est un principe fondamental de la loi sur la protection des renseignements personnels. Il s'agit d'un principe renforcé par le Règlement général sur la protection des données de l'Union européenne, dont la commissaire Denham vient de parler, et qui entrera en vigueur en Europe dans quelques jours seulement.

Vous serez peut-être intéressés d'apprendre que mon bureau mène actuellement une vaste enquête sur la façon dont les partis élus de notre assemblée législative recueillent et utilisent les renseignements personnels des électeurs. Je signale que ces partis ont pleinement collaboré à l'enquête de notre bureau. Je m'attends à ce qu'elle aboutisse à des recommandations et à des directives qui aideront les partis à améliorer leurs pratiques en matière de protection des renseignements personnels.

Bien entendu, je sais que les modifications proposées récemment à la Loi électorale du Canada obligeront les partis politiques à adopter une politique de protection des renseignements personnels et à la fournir au directeur général des élections. Ces propositions ne sont qu'un petit pas en avant. Elles sont une tentative d'inclusion du principe de la transparence, mais ce n'est là qu'un élément d'un régime adéquat de protection des données.

● (0905)

Les modifications proposées n'obligent pas les partis à répondre à la demande d'un électeur pour obtenir l'information qu'ils détiennent à son sujet et elles ne lui donnent pas non plus le droit de demander à un parti de corriger des renseignements inexacts à son sujet. Ce qui est peut-être le plus important, c'est qu'il n'y a aucune disposition permettant à un tiers impartial d'entendre et de trancher une plainte d'un électeur. Ces normes juridiques fondamentales font partie du droit de la Colombie-Britannique depuis des années et sont la norme dans de nombreuses démocraties occidentales. Les partis politiques ne devraient reculer devant aucune de ces obligations juridiques. En fait, leur mise en œuvre ne fera qu'accroître la confiance des citoyens dans leurs institutions démocratiques.

Je termine là-dessus, monsieur le président. Je serai heureux de répondre à vos questions.

Le président: Les membres du Comité savent qu'ils disposeront d'un certain temps pour la période publique de questions et que, après la première ronde de questions de cinq minutes, nous siégerons à huis clos. Je le dis pour que vous soyez prêts.

Nous allons commencer par M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour à vous deux. Bon après-midi, je suppose, en Angleterre. Merci beaucoup de vous être joints à nous.

Monsieur McEvoy, je vais commencer par vous.

La BBC a rapporté il y a quelques semaines qu'elle avait tenté de faire la visite des bureaux d'AIQ à Victoria. Elle avait trouvé les bureaux plutôt déserts, avec quelques personnes qui y travaillaient. Votre bureau a-t-il tenté de communiquer avec les directeurs d'AIQ qui sont impliqués dans cette affaire ou avez-vous essayé, de quelque façon, de visiter ces bureaux?

M. Michael McEvoy: Oui. Nous sommes bien engagés avec AggregateIQ en ce moment. Je ne veux pas dire grand-chose de plus. Nous sommes loin d'avoir terminé nos interrogatoires avec AggregateIQ.

Je pense que je vais en rester là.

M. Raj Saini: D'accord.

Madame Denham, j'ai quelques questions à vous poser.

Il y a une chose qui me préoccupe, qui se passe actuellement en Angleterre. Cambridge Analytica a déclaré faillite, et l'entreprise qui en est sortie s'appelle Emerdata. Il y a une autre entreprise qui s'appelle Firecrest Technologies. Il semble que les mêmes acteurs sont en train de se réaligner. Vous avez essayé d'obtenir un mandat, et je crois que vous l'avez demandé en vertu de la loi sur la protection des données de Blighty. Les personnes concernées avaient sept jours pour contester le mandat. Elles savaient que votre bureau faisait enquête ou allait les poursuivre.

Quand il est question d'une entreprise, qu'il s'agisse d'une entreprise de vente au détail ou d'une entreprise de fabrication, si on déplace les actifs matériels de cette entreprise ailleurs, il y a certains comptes à rendre, parce qu'on peut voir les bureaux, la machinerie, les produits, être déplacés. Mais quand il est maintenant question de données. Les données peuvent être acheminées très rapidement. Elles peuvent se trouver ailleurs, être utilisées d'autres façons. Si une entreprise veut redémarrer, elle a besoin d'un produit, et son produit, ce sont des données.

Avez-vous l'impression qu'il est maintenant difficile de savoir où sont allées ces données, sachant que les entreprises ont, d'une façon ou d'une autre, opéré un réalignement?

Mme Elizabeth Denham: Pour revenir à ce que vous avez dit au sujet du mandat, je conviens avec vous que les dispositions actuelles de la loi ne nous permettent pas de procéder rapidement avec un mandat. Nous devons être en mesure de traiter les cas de cybercriminalité et tout autre délit lié aux données. Les modifications que le gouvernement vient d'apporter à la loi nous conféreront de nouveaux pouvoirs qui nous permettront de réagir plus rapidement, sans être obligés de donner des préavis longtemps d'avance aux organisations. Cela dit, nous avons réussi à saisir de grandes quantités de données chez Cambridge Analytica et nous avons exécuté deux autres mandats dans le cadre de cette enquête. Nous avons donc beaucoup d'information en main. S'il existe des liens entre une compagnie et une autre et si leur propriété intellectuelle et leurs données sont utilisées par une nouvelle compagnie, nous pourrons alors faire enquête et poursuivre nos travaux. Si une compagnie déclare faillite, comme dans ce cas-ci, nous restons en contact avec les administrateurs et nous pouvons prendre des mesures d'exécution, tant au criminel qu'au civil.

M. Raj Saini: Vous savez évidemment que les responsables d'AIQ ont témoigné devant notre comité. Depuis leur comparution, l'entreprise coopère-t-elle davantage avec votre bureau?

Mme Elizabeth Denham: Nous avons récemment reçu une lettre d'AIQ qui laisse présager une meilleure coopération que celle que nous avons eue jusqu'à présent. J'ignore si c'est le résultat du témoignage devant votre comité et des discussions que vous avez eues; cela reste à voir. Les actes en diront plus que les paroles. Si nous n'obtenons pas leur coopération, comme je l'ai dit devant le comité parlementaire britannique, je prendrai d'autres mesures et recours juridiques.

● (0910)

M. Raj Saini: Cela m'amène à ma dernière question. Nous avons appris par *The Gardian* que vous examinez divers recours juridiques pour obliger AIQ à être plus coopérative. Pouvez-vous nous donner une idée des mesures que vous pourriez prendre?

Mme Elizabeth Denham: Je préférerais ne pas répondre à cette question sur la place publique, mais je vous dirai que nous étudions également des options en collaboration avec nos collègues canadiens engagés dans cette enquête.

M. Raj Saini: Combien de temps me reste-t-il?

Le président: Vous avez 30 secondes.

M. Raj Saini: Merci.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): J'ai une brève question à poser.

Notre actuel commissaire à la protection de la vie privée est loin d'avoir les mêmes pouvoirs que vous deux. Croyez-vous qu'il est important, surtout dans le contexte du scandale Facebook et Cambridge Analytica, que notre commissaire ait des pouvoirs accrus d'exécution de la loi, ne serait-ce que celui d'imposer des amendes et même d'infliger des sanctions pénales, des pouvoirs beaucoup plus larges que ceux qu'il détient actuellement?

Ma question s'adresse à vous deux.

Mme Elizabeth Denham: Si vous me permettez de commencer, je dirais que les pouvoirs du commissaire à la protection de la vie privée du Canada sont moins étendus qu'ailleurs dans le monde. Lorsque nous avons affaire à des entreprises internationales de données et que nous devons faire enquête rapidement, il est très important, à mon avis, d'être en mesure de rendre des ordonnances, d'imposer des pénalités administratives, des amendes et, surtout de saisir du matériel et d'agir rapidement.

Même les pouvoirs que je détiens en vertu de la Data Protection Act du Royaume-Uni ne suffisent pas dans ce cas-ci. Le gouvernement a réagi très rapidement et déposé des modifications, qui ont été adoptées hier soir, afin de nous donner des pouvoirs accrus de faire des inspections sans préavis, d'utiliser des mandats simplifiés, de rendre des ordonnances d'urgence et aussi d'infliger des sanctions pénales pour destruction de dossiers et de renseignements.

Dans le contexte général des entreprises numériques, il est important de pouvoir agir rapidement dans l'intérêt public.

Le président: Monsieur McEvoy, rapidement.

M. Michael McEvoy: Notre bureau a officiellement signifié qu'il est favorable à ce que le Parlement renforce les pouvoirs du Commissariat à la protection de la vie privée du Canada.

Je pense que nous devons y réfléchir dans l'intérêt des citoyens. Compte tenu des affaires sur lesquelles vous enquêtez, les Canadiens veulent avoir l'assurance qu'une entité investie d'un pouvoir réglementaire veille à leurs intérêts. Cela sera possible que si l'organisme de réglementation détient le pouvoir de s'assurer que les problèmes de ce genre seront corrigés efficacement s'ils suscitent des inquiétudes ou s'il y a transgression de la loi.

Le président: Monsieur Gourde, vous avez cinq minutes.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président. Je remercie nos deux témoins.

Ma première question s'adresse à Mme Denham, mais M. McEvoy pourra répondre aussi, s'il le désire.

Madame la commissaire, vous avez attiré notre attention sur les crimes liés à l'utilisation de données et au profilage.

Il semble y avoir un flou législatif quant à l'utilisation qui est faite de données prises sur Facebook. On crée des catégories de gens afin de pouvoir les cibler à des fins publicitaires ou pour les inciter à voter dans un sens ou dans l'autre. L'argument invoqué pour justifier l'utilisation de ces données est que les gens ont mis volontairement cette information sur leur profil Facebook.

Les gens consentent à indiquer sur leur profil qu'ils sont mariés, qu'ils ont des enfants ou qu'ils ont un véhicule rouge ou bleu, par exemple. Ces compagnies vont demander quel crime il y a à catégoriser tous les gens qui ont un véhicule bleu? Comment peut-on dire qu'il y a eu un crime lié aux données ou au profilage si ces données ont seulement servi à cibler des gens pour une simple publicité?

[*Traduction*]

Mme Elizabeth Denham: En vertu de la loi britannique et, en fait, de la loi sur la protection des données appliquée à la grandeur de l'Union européenne, les données doivent être recueillies et utilisées dans un but précis. Par exemple, si quelqu'un répond à un questionnaire en pensant qu'il communique des renseignements dans un but précis, disons dans le cadre d'une recherche universitaire, et que ces données sont ensuite utilisées à une autre fin, par exemple pour une campagne politique ou à des fins de profilage en fonction des goûts ou des penchants politiques de la personne, ce serait une infraction en vertu de la loi britannique. C'est exactement ce sur quoi portent nos enquêtes.

Si quelqu'un communique des renseignements personnels dans une application ou dans les médias sociaux, il doit y avoir un avis et une indication claire quant à l'utilisation qui sera faite de ces renseignements, à défaut de quoi, il y a infraction à la loi.

Au début de mon intervention, j'ai dit que les renseignements personnels recueillis aux fins de connaître les opinions ou les allégeances politiques sont classés dans une catégorie spéciale et ne peuvent être utilisés qu'avec le consentement explicite de la personne. Encore là, cette question est au coeur de notre enquête au Royaume-Uni.

● (0915)

M. Michael McEvoy: Si vous décidez de partager certains renseignements avec vos amis, cela ne veut pas dire que tout le monde peut les utiliser. On peut comprendre que si un utilisateur de Facebook exprime un intérêt pour les autos rouges, il recevra de la publicité sur les autos rouges. Une personne est toutefois loin de s'attendre à ce qu'on établisse son profil psychologique et qu'on la cible pour une publicité en particulier, parce qu'elle a été classée dans la catégorie des personnes ouvertes, névrosées ou autre. Je pense que cela dépasse largement les attentes du citoyen moyen et que cela va à l'encontre de la loi sur la protection de la vie privée.

[*Français*]

M. Jacques Gourde: Y a-t-il des études ou des données qui prouvent que le profilage est vraiment très efficace dans certaines situations et qu'il peut changer le cours de l'histoire, ou cela fait-il simplement partie de la joute politique d'aujourd'hui? Peut-être aurons-nous le devoir de légiférer à cet égard, mais nous devrons aussi travailler en utilisant le profilage, parce que cela existe depuis une dizaine d'années maintenant. Cela n'existait pas avant. Auparavant, on le faisait peut-être de façon moins méthodique. Cependant, aujourd'hui, les moteurs de recherche et les possibilités informatiques permettent de réaliser ce genre de recherche.

De quelle façon envisagez-vous l'avenir, compte tenu de cette nouvelle réalité?

[*Traduction*]

Mme Elizabeth Denham: Lorsque je parle aux responsables des partis politiques, et nous avons parlé à ceux des principaux partis politiques et campagnes au Royaume-Uni, je pense que c'est ce qu'ils recherchent, tout en sachant qu'ils devront élargir leur recherche et peut-être faire du ciblage plus précis pour rejoindre les partisans potentiels et existants. Il est possible que les technologies nous aient échappé.

Pour maintenir la confiance des électeurs, il est vraiment important de respecter les principes du droit, comme la reddition de comptes et la transparence. Ce n'est pas parce que nous avons de nouvelles méthodes de recherche, ou parce que les gens prétendent qu'elles sont plus efficaces pour attirer des partisans potentiels, que c'est correct de les utiliser.

Nous devons nous demander s'il y a, dans le monde d'aujourd'hui, des lignes à ne pas franchir pour ce genre de pratiques secrètes de jumelage de données ou de profilage. C'est maintenant qu'il faut agir, parce que si nous n'adoptons pas cette politique gouvernementale dès maintenant, nous risquons de perdre la confiance des gens au fur et à mesure que ces techniques deviendront plus efficaces et plus accessibles.

Dans mon rapport, je recommanderai notamment l'application d'un code de conduite portant expressément sur l'analyse de données dans le contexte politique.

Le président: Merci, monsieur Gourde.

Nous passons maintenant à vous, monsieur Angus. Vous avez cinq minutes.

M. Charlie Angus (Timmins—Baie James, NPD): Merci beaucoup d'être venus aujourd'hui.

Madame Denham, notre comité a entendu les témoignages de MM. Massingham et Silvester. Avez-vous pris connaissance de leurs témoignages?

Mme Elizabeth Denham: Oui, je l'ai fait.

M. Charlie Angus: Nous cherchions à déterminer quel était le lien entre SCL et AggregateIQ. M. Massingham a catégoriquement affirmé qu'il n'y avait aucun lien, ce qui semblait contredire les documents que nous avions obtenus. Croyez-vous qu'il nous a tout dit dans son témoignage?

Mme Elizabeth Denham: Nous avons posé des questions très précises à AggregateIQ dans le cadre de notre enquête et, comme je l'ai dit tout à l'heure à votre collègue et comme je l'ai aussi dit publiquement, nous attendons encore des réponses exhaustives.

Nous examinons également une pléthore de documents qui nous ont été fournis pour notre enquête, comme des déclarations de témoins, des renseignements communiqués par des dénonciateurs et d'autres documents qui nous ont été soumis. C'est l'une des questions au coeur de notre enquête. Nous espérons aller au fond de cette affaire.

● (0920)

M. Charlie Angus: Merci.

Monsieur McEvoy, vous semblez très déterminé à assujettir les partis politiques à la Loi sur la protection des renseignements personnels et les documents électroniques. Nous, les élus, nous ne sommes pas très enclins à parler des données que nous recueillons. Nous les protégeons jalousement.

Lorsque j'ai été élu, j'ai compris que le gros de mon travail se faisait dans ma circonscription. Nous avons affaire à des immigrants, des gens qui font faillite. Les gens viennent nous voir pour des problèmes médicaux, des problèmes d'expulsion, de protection de l'enfance. Nous recueillons une quantité de renseignements très personnels. À mon bureau, personne n'a reçu de formation sur la collecte de renseignements. Nous avons un code rigoureux. Je suppose que c'est ce que font tous les députés à leurs bureaux de circonscription. J'ai eu affaire avec quelques bureaux de députés d'autres partis sur certains cas sensibles. Nos rapports ont toujours été très professionnels, mais nous recueillons ces données seulement pour aider nos électeurs. Nous tenons toujours des dossiers distincts ou un ensemble de données distinct pour les élections, mais il va sans dire que ces données pourraient être mélangées si nous n'avions pas certaines lois ou certaines exceptions. À votre avis, pour avoir la confiance des gens qui font appel à nos services, serait-il souhaitable qu'ils sachent que nous sommes assujettis à une loi fédérale visant la protection des données personnelles?

M. Michael McEvoy: Il est important que les Canadiens comprennent que leurs renseignements personnels sont correctement protégés.

Je ferais cependant une distinction. Vous parlez surtout du travail que vous effectuez pour vos électeurs. En Colombie-Britannique, la plupart de ces renseignements seraient exemptés en vertu de la loi sur l'accès à l'information.

M. Charlie Angus: Oui.

M. Michael McEvoy: Ce dont nous parlons maintenant, c'est de l'activité des partis politiques et de la collecte de données.

En y réfléchissant bien, je pourrais répondre autrement à votre question. En Colombie-Britannique, nous avons eu l'occasion d'enquêter sur des cas où la collecte de renseignements par le parti au pouvoir a donné lieu à des allégations selon lesquelles le parti aurait franchi une ligne, ou se serait retrouvé dans une zone grise, et qu'il aurait prétendument transféré ces renseignements à des sources du parti.

Si nous n'avions pas eu le pouvoir d'enquêter sur les partis, l'enquête se serait terminée là. Je pense que cela aurait été non seulement problématique pour notre propre enquête, mais aussi parce que le public n'aurait jamais su ce qui est vraiment arrivé aux renseignements recueillis. Comme la loi nous permet d'enquêter sur les partis politiques, nous avons pu effectuer un examen global et en arriver à des conclusions quant à ce qui a pu arriver à ces renseignements. Je crois que cela a renforcé la confiance du public dans le fait que les renseignements ont été traités de manière appropriée. Si cela n'avait pas été le cas, notre bureau aurait pu imposer des sanctions.

M. Charlie Angus: Oui, je pense que c'est important. Encore une fois, dans le cadre de notre travail dans nos bureaux de circonscription, nous traitons des données très... C'est sacré. Je dis toujours à mon équipe que tout ce qui se dit dans ce bureau, c'est comme au confessionnal: cela ne doit jamais sortir de là. Il est important d'avoir cette confiance. Les gens viennent nous voir et nous confient des détails très intimes de leur vie. Trois semaines plus tard, nous leur téléphonons pour leur demander de prendre une affiche électorale. Ces personnes doivent avoir l'assurance que nous n'utilisons pas leurs données personnelles dans le but de placer nos affiches électorales. C'est un code d'honneur.

Serait-il préférable d'avoir un code juridique très clair pour rassurer les citoyens, en cette époque de perte de confiance envers la classe politique, afin qu'ils sachent qu'au Canada, ils peuvent divulguer des renseignements personnels aux élus en toute confiance. Les données qu'ils nous confient à des fins politiques pourront être partagées, mais celles qu'ils ne souhaitent pas que nous partagions ne le seront pas.

M. Michael McEvoy: C'est un exemple intéressant. Si quelqu'un alléguait que les données ont été détournées vers le parti politique, comme vous le décrivez, la capacité de l'organisme de réglementation... Je pense que la confiance du public dans le système pourrait être renforcée si les gens savaient qu'un organisme pourra faire enquête pour déterminer si le parti a recueilli des renseignements qu'il n'aurait pas dû recueillir. Là encore, il incombe aux législateurs de déterminer qui doit détenir ce pouvoir de surveillance au Canada. Je sais que le Commissariat à la protection de la vie privée doit prendre en compte certains enjeux constitutionnels ou juridiques. En Colombie-Britannique, il est arrivé à mon bureau de s'occuper de certaines affaires qui ne cadraient pas parfaitement avec notre mandat, mais qui peuvent lui être confiées aux fins d'arbitrage.

De même, quant à savoir s'il s'agit d'une instance appropriée, d'une loi appropriée pour assujettir les partis politiques aux dispositions sur la protection de la vie privée et la protection des données... il se peut que la Loi sur la protection des renseignements personnels et les documents électroniques ne soit pas le bon outil, je ne sais pas. Encore là, c'est aux législateurs qu'il revient de déterminer cela. Cependant, le commissaire à la protection de la vie privée du Canada pourrait se prononcer sur ces affaires, parce qu'il est bien placé pour cela. Il a l'expertise et le personnel. Il a un pouvoir d'enquête sur ce genre de questions.

● (0925)

M. Charlie Angus: Je vous remercie.

Le président: Merci, monsieur Angus.

Les cinq dernières minutes sont à vous, monsieur Baylis.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Je vous remercie, monsieur le président.

Madame Denham, merci de votre présence.

De toute évidence, AIQ inquiète autant les législateurs que les citoyens canadiens. C'est le point de départ pour nous, parce que nous ne voulons pas que les gens utilisent le Canada comme un abri pour mener des activités illégales ailleurs. Les responsables sont venus témoigner devant le Comité. Comme vous l'avez constaté, nous en sommes arrivés à la conclusion qu'ils ne nous ont pas tout dit. Je dirais même qu'ils ont peut-être délibérément essayé de nous induire en erreur. Ils font partie d'un groupe de compagnies. Ils font partie de Cambridge Analytica, de SCL... À un moment donné, leur entreprise s'appelait SCL Canada.

De plus, l'affaire débute avec Aleksandr Kogan et Global Science Research. C'est lui qui a recueilli toutes ces données. A-t-il violé l'une de vos lois? Vous êtes-vous prononcés là-dessus?

Mme Elizabeth Denham: Nous enquêtons sur M. Kogan et sur son application. Nous examinons comment elle fonctionnait, son lien avec Cambridge Analytica et ce qui s'est vraiment passé sur le terrain avec cette application.

Comme M. Kogan a refusé de collaborer à notre enquête, nous prenons donc d'autres mesures dans le but d'obtenir une déclaration de lui. Nous avons des outils d'exécution de la loi. Nous avons des recours civils, mais c'est une importante piste d'enquête pour nous au Royaume-Uni.

M. Frank Baylis: Je ne suis pas surpris que M. Kogan ne coopère pas. Supposons qu'il soit parti en emportant ces données. Ce serait du vol. Quand vous disparaissez par la porte arrière, en emportant quelque chose qui ne vous appartient pas, vous enfreignez les règles. Je dirais que M. Kogan a volé ces données.

Nous devons donc nous demander pourquoi M. Steve Bannon ferait le déplacement des États-Unis jusqu'en Europe, jusqu'au Royaume-Uni pour s'entretenir avec SCL et participer à la création de Cambridge Analytica? Ces compagnies possédaient-elle des capacités particulières ou avaient-elles simplement accès à ces données?

Avez-vous parlé à M. Bannon? Avez-vous l'intention de lui parler dans le cadre de votre enquête?

Mme Elizabeth Denham: Je le répète, je ne peux répondre à cela parce que l'enquête est en cours. Je ne veux formuler aucune hypothèse quant à la raison pour laquelle la compagnie a été structurée de cette façon. C'est une question que se posent certainement les comités parlementaires des deux côtés de l'Atlantique, ainsi que les procureurs généraux et d'autres organismes de réglementation.

M. Frank Baylis: Cela semble très intéressant parce Facebook, Google et une foule de ces compagnies très puissantes et performantes sont implantées et exercent leurs activités aux États-Unis, mais elles ont jugé nécessaire d'aller au Royaume-Uni. Le seul endroit où ces gens vont est justement celui qui a accès aux données que M. Kogan a colligées, et il refuse de coopérer en nous disant comment il les a obtenues.

Nous revenons à M. Kogan, qui a été financé dans le passé, si j'ai bien compris, par le gouvernement russe et des branches du gouvernement russe. Nous constatons que le régime russe, sous Vladimir Poutine, est intervenu dans des élections. Est-il possible que M. Bannon soit allé là-bas pour mettre à l'essai sur le vote du Brexit le stratagème qu'il avait l'intention d'utiliser six ou sept mois plus tard dans l'élection américaine? Est-ce une possibilité?

Mme Elizabeth Denham: Je vous rappelle que notre enquête concerne avant tout la collecte, l'utilisation et la prétendue utilisation abusive de données personnelles par Cambridge Analytica et SCL dans le contexte des élections. Il incombe à d'autres d'établir ces liens à l'international.

Nous obtiendrons des réponses aux questions que nous avons dans le cadre de notre enquête en vertu de la loi sur la protection des données du Royaume-Uni.

M. Frank Baylis: Vous nous avez été d'une grande utilité et nous avons coordonné notre enquête avec celle du Royaume-Uni. Est-ce qu'un représentant du gouvernement américain a communiqué avec vous pour vous aider à coordonner votre enquête, un peu comme nous le faisons?

● (0930)

Mme Elizabeth Denham: Nous avons communiqué avec nos collègues américains dans le cadre de cette enquête. Je n'ai pas eu de contact avec le Congrès ni avec des élus. C'est une question qu'il faudrait poser à Damian Collins et au Comité spécial de la culture, des médias et du sport du Royaume-Uni.

M. Frank Baylis: J'ai l'impression que certains éléments britanniques ont collaboré ou travaillé avec un pouvoir étranger hostile — et j'entends par là le régime de Vladimir Poutine — dans le but de saper notre démocratie. Dans le passé, nous aurions parlé de trahison et ces personnes auraient été jugées en conséquence.

Si jamais ces liens s'avéraient, allez-vous transmettre l'information à cette instance?

Mme Elizabeth Denham: En vertu de la loi qui régit mon organisme, je peux transmettre des renseignements à d'autres organismes chargés de l'application de la loi ou à des organismes de réglementation si je juge que c'est dans l'intérêt public.

Par exemple, j'ai transmis à la Commission électorale du Royaume-Uni des renseignements qui, selon moi, se rapportaient à ses enquêtes sur le financement des campagnes. C'est en mon pouvoir de le faire. S'il m'arrivait de trouver d'autres renseignements qui seraient pertinents dans le cadre d'une enquête sur l'application de la loi, alors j'ai la capacité, en vertu de cette loi, de communiquer ces renseignements.

Le président: Merci, monsieur Baylis.

Avant de passer à huis clos, je tiens à vous remercier de votre collaboration, du point de vue de notre comité, et je suis impatient de poursuivre cette collaboration. Nous examinons également toutes les options juridiques que le Comité peut envisager si des problèmes survenaient à la suite des témoignages qui y ont été entendus.

●

_____ (Pause) _____

●

● (0955)

Le président: Nous reprenons nos travaux. Je m'excuse de ce changement rapide et du peu de temps dont nous disposons pour nous installer.

Je remercie particulièrement nos témoins d'aujourd'hui. Colin McKay est chef des politiques publiques et des relations gouvernementales chez Google Canada. Nous nous sommes déjà rencontrés. Nous accueillons M. Jim Balsillie, du Conseil des innovateurs canadiens.

Bienvenue.

En raison de notre temps limité, les déclarations préliminaires seront de cinq minutes.

Nous allons commencer par M. McKay de Google. Merci.

M. Colin McKay (chef, Politiques publiques et relations gouvernementales, Google Canada): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invité à comparaître aujourd'hui. C'est un plaisir de vous parler de nouveau de ces sujets importants.

Je tiens également à souligner qu'aujourd'hui est un jour particulièrement chargé d'émotion pour le Parlement. J'ai eu la chance de passer du temps avec Gord Brown, sur la Colline et ailleurs, et je sais qu'il nous manquera.

Google travaille fort pour offrir à ses utilisateurs du choix, de la transparence, un bon encadrement et de la sécurité. Nous sommes heureux d'avoir l'occasion de vous parler de la façon dont nous protégeons les Canadiens ainsi que nos milliards d'utilisateurs dans le monde. J'ai pensé qu'une petite mise en contexte sur la présence de Google au Canada serait utile à cette conversation.

Pour une entreprise qui n'a que 20 ans, Google a de profondes racines canadiennes. Il y a 16 ans, Google choisissait d'établir son premier bureau international au Canada. Depuis, nous sommes passés à plus de 1 000 employés au Canada, dont plus de 600 programmeurs et chercheurs en intelligence artificielle à Montréal, Waterloo et Toronto. Notre mission est d'organiser l'information mondiale et de la rendre universellement accessible et utile. Les services de Google offrent des avantages réels aux Canadiens, qu'il s'agisse de Search, Maps, Translate, Gmail, Android, Cloud ou encore de nos appareils, tous nos produits aident les gens à obtenir des réponses, à organiser leur information et à rester branchés.

Nos produits publicitaires aident les entreprises canadiennes à joindre des clients partout dans le monde et nos outils de recherche aident les Canadiens à trouver de l'information, des réponses et même des emplois. Il y a quelques semaines à peine, nous avons mis en place de nouvelles façons pour les Canadiens de trouver un emploi au moyen de Google Search.

Comme vous le savez peut-être, Google a beaucoup investi dans l'écosystème florissant de l'intelligence artificielle du Canada, non seulement en finançant des organisations comme MILA à Montréal et Vector à Toronto, mais aussi en établissant des laboratoires de recherche qui ont aidé le Canada à attirer et à retenir des collaborateurs de calibre mondial.

Nos ingénieurs travaillent sur des produits importants comme Gmail, le navigateur Chrome et Cloud, des produits utilisés par des milliards de personnes dans le monde entier. Nous avons une équipe canadienne qui travaille à mettre au point une technologie de navigation sécuritaire qui prévient les attaques de maliciels et les escroqueries par hameçonnage, tout en assurant la sécurité du Web ouvert.

Cela m'amène à vous dire que Google réfléchit depuis longtemps à la protection de la vie privée et à la sécurité. Au cours des cinq dernières années, Google a investi dans ses outils et dans ses équipes afin d'offrir aux utilisateurs du choix, de la transparence et une sécurité de premier ordre en ce qui a trait à leurs données. Nous offrons des outils comme Mon compte, Security Checkup, Privacy Checkup, Google Takeout, Google Play Protect et plus encore, tous conçus dans le but de protéger les données des utilisateurs, de leur permettre de prendre facilement des décisions éclairées en matière de protection de la vie privée et de leur donner la possibilité de transférer facilement leurs données sur d'autres plateformes.

En 2015, nous avons lancé Mon compte, ou myaccount.google.com, qui offre aux utilisateurs canadiens un outil centralisé rapidement accessible et convivial qui leur permet d'exprimer leurs préférences en matière de vie privée et de sécurité. Il est très utilisé. Cet outil a reçu plus de deux milliards de visites dans le monde en 2017, dont des dizaines de millions de la part de Canadiens. Nous continuons de promouvoir l'utilisation de cet outil, mais il est clair que la sensibilisation prend de l'ampleur et que les Canadiens l'utilisent pour faire des choix éclairés.

Google fait la promotion de Privacy Checkup, l'outil de vérification des paramètres de confidentialité, auprès des utilisateurs de façon récurrente afin d'aider ceux-ci à tenir leurs paramètres à jour en matière de protection de la vie privée à mesure qu'évolue leur utilisation des services de Google. Les utilisateurs peuvent voir les types de données que Google recueille, examiner les renseignements personnels qu'ils partagent et choisir les types d'annonces qu'ils aimeraient que Google leur montre. De plus, nous avons un outil appelé Security Checkup qui aide les utilisateurs à comprendre quels appareils et quelles applications ont accès à leurs données.

Sur nos plateformes Android sous licence Google, nous avons développé Google Play Protect, qui protègent les appareils contre les applications malveillantes. Nous concevons nos produits et mettons en œuvre des politiques de produits de façon à protéger prioritairement les renseignements personnels des utilisateurs. Cela fait partie de notre engagement: nous veillons à ce que nos utilisateurs comprennent la façon dont nous utilisons les données pour améliorer leur expérience avec les produits et services de Google. Il est difficile de garantir que les données demeurent privées si elles ne sont pas protégées, ce qui explique en partie pourquoi, chez Google, nous avons mis sur pied une équipe de sécurité aussi solide. C'est aussi la raison pour laquelle nous avons non seulement mis l'accent sur la sécurité de Google et de ses services, mais nous avons aussi aidé l'ensemble de l'industrie de l'Internet à renforcer la sécurité, grâce à notre leadership avec des projets comme la navigation sécuritaire, HTTPS Everywhere, le cryptage des courriels en transit et notre leadership dans la promotion de clés d'authentification sécuritaires à deux facteurs.

Nous savons que nos utilisateurs sont des personnes. Ce sont des membres de la famille, des amis et des voisins. Certains comptent sur nos produits pour bâtir leur entreprise et celles-ci sont sans but lucratif. D'autres ont simplement besoin d'aide pour trouver un produit, une adresse ou les heures d'ouverture d'un commerce, mais chacun d'entre eux nous fait confiance, et nous reconnaissons l'énorme valeur de la confiance que les Canadiens nous accordent.

Je vous remercie encore une fois de m'avoir donné l'occasion de m'adresser à vous aujourd'hui et je me ferai un plaisir de répondre à vos questions.

● (1000)

Le président: Merci, monsieur McKay.

C'est maintenant au tour de M. Balsillie, pour cinq minutes.

Me Jim Balsillie (président, Conseil des innovateurs canadiens): Merci.

Monsieur le président, mesdames et messieurs les membres du Comité, j'ai suivi votre comité de près parce que je crois que les Canadiens sont aux prises avec la plus importante question de politique publique de notre époque, soit la gestion des données.

Les innovateurs canadiens savent que les flux de données ont transformé le commerce, qu'ils ont fait des données l'actif le plus précieux de l'économie actuelle, qui est elle-même une économie axée sur les données. Les entreprises utilisent les données pour créer de nouveaux marchés et y accéder ainsi que pour interagir à l'échelle mondiale avec les clients et les fournisseurs. Le fait d'avoir la mainmise sur les données et les réseaux permet aux entreprises dominantes d'entraver la concurrence, d'obtenir des rentes de monopole de leurs clients et de tromper les consommateurs par leurs stratégies de collecte de données. De grandes quantités de données sont recueillies et gérées par des infrastructures numériques étrangères non réglementées. C'est la raison pour laquelle le Conseil des innovateurs canadiens a demandé à nos gouvernements de concevoir une stratégie nationale des données, de façon à s'assurer que les flux transfrontaliers de données et d'information servent les intérêts de l'économie canadienne.

Une stratégie nationale en matière de données devrait faire en sorte de systématiser le traitement de la concurrence dans les sections des accords de libre-échange portant sur les données, y compris le droit à un accès concurrentiel aux données qui circulent sur de grandes plateformes et qui possèdent un statut de facto de service public. Si le Canada ne crée pas des lois adéquates sur l'hébergement, la localisation et l'acheminement des données qui protègent les Canadiens, alors nos données sont assujetties aux lois étrangères, ce qui fait du Canada un État client.

Bien que les scandales de Facebook aient provoqué la récente série de témoignages devant ce comité, je vous exhorte à vous armer de faits au sujet de l'économie des données, qui est complètement différente de l'économie fondée sur le savoir qui l'a précédée et de l'économie axée sur la production du XX^{e} siècle.

Ces données intangibles marchandisées ne sont pas régies de la même façon que les biens tangibles. L'économie axée sur les données tire sa valeur de la collecte, du repérage, de la marchandisation et de l'utilisation des flux de données.

Ce que nous avons entendu de la part d'entreprises comme Facebook, devant ce comité notamment, dresse un portrait inexact de la réalité. Le scandale de Cambridge Analytica et de Facebook n'est pas une atteinte à la vie privée ni une question de gouvernance d'entreprise. Ce n'est même pas une question de confiance. C'est une question de modèle d'entreprise fondé sur l'exploitation des lacunes actuelles des lois canadiennes en matière de gouvernance des données.

Facebook et Google sont des entreprises fondées exclusivement sur le principe de la surveillance de masse. Leurs revenus proviennent de la collecte et de la vente de toutes sortes de données personnelles, dans certains cas sans conscience éthique. Par exemple, en Australie, Facebook s'est fait prendre à vendre l'accès à des données à des enfants suicidaires et vulnérables.

Le capitalisme de surveillance constitue actuellement la plus importante force du marché et c'est pourquoi les six entreprises les plus chèrement évaluées sont toutes axées sur les données. Leur dynamique unique exige une approche stratégique et souveraine propre au Canada, car les données et la propriété intellectuelle constituent à l'heure actuelle des déterminants clés de la prospérité, du bien-être, de la sécurité et de l'éthique.

Les données sous-tendent tous les aspects de notre vie, comme vous pouvez le voir dans l'illustration que je vous ai donnée en guise de cadre de référence. Par leur qualité d'actif incorporel, les données ont des effets non commerciaux essentiels. Dans cette optique, j'émets la recommandation suivante: mettre en oeuvre des dispositions inspirées du RGPD pour le Canada. Le RGPD offre de précieuses leçons et constitue un bon point de départ pour les législateurs et les organismes de réglementation du Canada. Il s'agit d'une avancée universellement reconnue en matière de protection de la vie privée et de contrôle des données.

Les décideurs politiques européens reconnaissent que quiconque contrôle les données contrôle également les personnes et les choses qui interagissent avec ces données, aujourd'hui et pour l'avenir. C'est pourquoi ils ont veillé à ce que les citoyens de l'Union européenne possèdent et contrôlent leurs données. De la même façon, les Canadiens devraient posséder et contrôler leurs données. Les Canadiens doivent acquérir des compétences officielles dans ce nouveau type d'économie, car elle touche tous les aspects de notre vie. Pour notre démocratie, notre sécurité et notre économie, les citoyens canadiens, et non les géants de la technologie multinationale qui n'ont de comptes à rendre à personne, doivent contrôler les données que nous et nos institutions générons.

En se concentrant uniquement sur la protection des renseignements personnels, les Canadiens peuvent se retrouver à ne colmater qu'une seule de nombreuses brèches, ce qui, dans les faits, n'aura aucun effet. Nous avons besoin d'une optique horizontale pour les lois et les politiques. La protection de la vie privée et les services numériques tant publics que privés ne sont pas en opposition. Par exemple, l'Estonie montre qu'une meilleure gouvernance des données entraîne une augmentation de la protection de la vie privée dans les services numériques.

Les économistes n'ont de cesse de démontrer que l'économie axée sur les données se développe à une vitesse plus rapide que la création de politiques fondées sur des données probantes. Je vous exhorte à travailler avec les innovateurs et les experts canadiens qui comprennent les technologies ouvertes, les sciences des données, la concurrence, l'établissement de normes, la réglementation stratégique, les accords commerciaux, l'éthique des algorithmes, l'IP et la gouvernance des données.

● (1005)

Nous avons besoin d'eux pour élaborer des politiques détaillées de nature technique. En travaillant avec des experts, nous pouvons faire progresser notre pays et veiller à ce que le Canada ne rate pas le train de l'économie des données, comme il a raté sa chance de prospérer dans l'économie du savoir au cours des 20 dernières années.

Sur le plan personnel, en tant que Canadien, je suis profondément préoccupé par l'effet qu'ont les entreprises de surveillance de masse sur la société canadienne et sur les Canadiens. Les renseignements personnels ont déjà été utilisés pour manipuler des personnes, leurs relations sociales et nuire à leur autonomie. Toutes les données recueillies peuvent être retraitées, utilisées et analysées ultérieurement, de façons qui ne peuvent être anticipées au moment de la collecte. Cela a des répercussions majeures sur notre liberté et notre démocratie.

Je crains que sans la conception et la mise en oeuvre d'une stratégie nationale sur les données, nos politiciens n'aillent de l'avant avec des initiatives d'entreprises étrangères qui font dans la surveillance de masse. Certaines de ces entreprises ont déjà démontré qu'elles savaient utiliser des données à des fins de manipulation. Malheureusement, l'histoire offre des leçons qui donnent à réfléchir sur les sociétés qui pratiquent la surveillance de masse.

C'est le rôle d'un gouvernement libéral et démocratique d'améliorer la liberté en protégeant la sphère privée. La sphère privée est ce qui nous rend libres. Il n'y a pas de consentement ou de retrait individuel à une ville ou à une société qui pratique la surveillance de masse, et c'est la voie que le Canada suit actuellement. Par conséquent, en plus de mettre en place des structures d'incitation économique et des cadres réglementaires appropriés, je vous exhorte, vous et vos collègues élus, à agir avec audace pour préserver nos valeurs démocratiques libérales, promouvoir l'intérêt public et affirmer notre souveraineté nationale.

Je vous remercie de tenir compte de mes recommandations et de me donner l'occasion de témoigner aujourd'hui.

● (1010)

Le président: Merci à vous deux, Colin et M. Balsillie, de vos témoignages.

Monsieur Picard, vous avez sept minutes.

[*Français*]

M. Michel Picard (Montarville, Lib.): Je vous remercie, messieurs McKay et Balsillie.

M. Balsillie a tenu quelques propos assez directs à l'égard de Google. Je vais donc inviter M. McKay à réagir aux allégations que M. Balsillie a faites dans son témoignage.

[*Traduction*]

M. Colin McKay: M. Balsillie a fait des recommandations très constructives quant à la nécessité d'une stratégie canadienne en matière de données, qui permette aux entreprises canadiennes de même qu'aux entreprises qui sont en concurrence sur le marché canadien de comprendre les données dont elles disposent et de mesurer les occasions d'affaires qui s'offrent à elles si elles veulent en tirer parti. Voilà l'occasion pour le gouvernement de créer une stratégie nuancée qui aide le Canada à se démarquer du reste du monde, non seulement dans le secteur de la technologie, mais également dans celui de la santé, où nous avons déjà une bonne longueur d'avance en ce qui concerne les renseignements médicaux, le secteur de l'agriculture, le secteur des mines et le secteur manufacturier.

Il n'est pas nécessaire qu'une stratégie en matière de données soit aussi restrictive ou prescriptive que l'a laissé entendre M. Balsillie. En fait, une stratégie qui tenterait d'isoler le Canada ou qui créerait des obligations qui ne sont pas semblables à celles qui existent ailleurs dans le monde limiterait les possibilités d'innovation offertes aux Canadiens, et ce, tant au Canada qu'à l'étranger. Tout cadre réglementaire doit être cohérent et prévisible.

Enfin, j'aimerais souligner que, malgré ce qu'a dit M. Balsillie, nous ne vendons pas les renseignements personnels de nos utilisateurs. Le modèle d'affaires que nous avons développé nous permet de fournir des services et des produits aux utilisateurs sur la base d'une relation personnelle et l'information que nos clients nous communiquent est utilisée pour leur fournir des services personnalisés.

Nous sommes en faveur de cette vaste gamme de services offerts gratuitement aux Canadiens et à beaucoup d'autres dans le monde grâce à la publicité. La publicité cible des segments de la population, pas des particuliers, et il n'y a pas d'échange de renseignements personnels entre Google et les annonceurs. Il s'agit simplement de reconnaître qu'une transaction économique doit être conclue pour offrir ces services, et la publicité est la façon la plus courante et la plus pratique de le faire à l'heure actuelle.

[*Français*]

M. Michel Picard: C'est exactement là que je veux en venir.

J'aimerais qu'on adopte une approche qui ne s'adresse pas aux initiés, mais plutôt une approche vulgarisée, si je puis dire, pour que les gens ou le public en général qui suivent les travaux du Comité comprennent.

Pour comprendre vraiment les tenants et aboutissants de ce que cela implique, je vais reprendre vos derniers commentaires. Tentons d'avoir une discussion qui soit axée exclusivement sur l'aspect commercial et non sur les grandes politiques et les grands concepts philosophiques.

Lorsque quelqu'un s'inscrit à Google, il ne remplit pas de formulaire en particulier, n'est-ce pas?

M. Colin McKay: Parlez-vous d'un formulaire particulier pour les services offerts par Google?

M. Michel Picard: Je ne suis pas obligé de remplir un formulaire qui comprend plusieurs données personnelles pour avoir accès au fureteur Google.

● (1015)

M. Colin McKay: Non.

M. Michel Picard: Comme vous avez peu ou pas de renseignements à mon sujet, ma première réaction serait de dire qu'il n'y a pas de renseignements me concernant qui pourraient être mis à risque.

M. Colin McKay: C'est vrai.

Il y a des niveaux d'expertise liés aux individus. Si vous vous inscrivez à un service offert par Google, on vous donne le service et on présume que vous êtes un homme d'un certain âge qui travaille à Ottawa. Lorsque vous utilisez notre service, nous pouvons voir que vous faites des recherches sur les résultats d'une partie de hockey, par exemple. Au cours de votre utilisation, on fait des suppositions quant aux choses que vous préférez et que vous cherchez fréquemment.

M. Michel Picard: D'accord.

Le fait que je préfère un genre de livre ou de site sportif, peu importe, n'est-ce pas là une préférence personnelle qui devient une information privée? À l'insu de l'utilisateur, on prend note de son utilisation du fureteur et on décide de son genre de comportement.

Si je comprends bien, vous vous tournez vers le marché privé et vous dites aux acheteurs de publicités que vous avez des cibles pour eux. C'est gentil de rendre un service gratuit, mais cela ne paie pas l'épicerie à la fin du mois.

[*Traduction*]

M. Colin McKay: Ce qu'il faut souligner, c'est que nous n'offrons pas un service qui permet aux annonceurs de cibler des personnes. Ce que nous disons, c'est que nous avons constaté que certains utilisateurs faisaient une recherche sur des parties de hockey et qu'ils pouvaient faire une recherche sur ces parties de hockey en inscrivant une équipe ou une province en particulier.

[*Français*]

M. Michel Picard: Vous rendez le service d'identifier l'individu parce que c'est vous qui possédez l'information fournie par l'adresse IP.

M. Colin McKay: Nous n'identifions pas l'individu.

[*Traduction*]

Pour l'annonceur, tout ce que nous disons, c'est: « Vous aimeriez faire une campagne publicitaire auprès des gens qui démontrent ces caractéristiques. Nous livrerons cette campagne de publicité. » Il ne sait pas qui voit les publicités. Ils ne reçoivent aucune information sur les personnes qui voient leurs publicités. Ils ont une idée du nombre de personnes et de certaines caractéristiques des personnes qui ont vu leurs publicités.

M. Michel Picard: Mais vous, vous le savez.

M. Colin McKay: C'est notre travail.

M. Michel Picard: C'est votre travail, mais vous savez qui a utilisé quoi, parce que vous avez les adresses IP. Vous connaissez la personne liée à l'adresse IP, mais vous devez prouver que la personne qui a saisi l'information est la même que celle qui est inscrite sur l'IP, mais il n'y a toujours pas d'ordinateur qui communique avec un site. C'est une personne qui le fait, et vous avez donc en main le lien manquant entre les renseignements personnels et les intérêts de tiers.

M. Colin McKay: J'ai mentionné Mon compte. Si vous voulez comprendre comment nous avons utilisé cette information et comment nous vous avons fourni des services, si vous allez sur Mon compte, vous pourrez voir une liste des attributs et des qualités que nous avons associés avec vous. Pour ce qui est de comprendre les renseignements que nous avons échangés dans le cadre de notre relation, nous l'indiquons clairement dans Mon compte.

Il n'est pas dans notre intérêt de faire quelque transaction que ce soit avec une tierce partie qui échangerait cette information. Le genre d'échange que nous faisons se décrit comme suit: si nous vous fournissons l'information souhaitée, nous pourrions en apprendre davantage sur votre besoin de trouver un stationnement près d'une partie de hockey à cause de la préférence que vous avez indiquée pour aller à des parties de hockey. Nous vous indiquerons donc, dans Maps, où se trouve le stationnement disponible le plus près.

M. Michel Picard: Merci.

Le président: Merci, monsieur Picard.

Le prochain intervenant est M. Gourde, pour sept minutes.

[*Français*]

M. Jacques Gourde: Je vous remercie, monsieur le président.

Ma question s'adresse à M. McKay.

Mardi, Google a annoncé que l'intelligence artificielle pourra bientôt converser au téléphone à notre place. Cela veut dire que mon assistant virtuel de Google pourra prendre pour moi un rendez-vous chez le coiffeur et le noter dans mon agenda personnel. Je n'aurai qu'à le lui demander et il le fera.

Ce qui m'inquiète à ce sujet, c'est que s'il est possible d'aller chercher une donnée concernant un tiers et de l'entrer dans son agenda personnel, ces mêmes robots pourront poser une multitude de questions à 100 000 personnes. Aimez-vous le bleu, par exemple? Ils pourraient poser sept, huit, neuf, dix, onze ou douze questions et faire l'analyse des réponses par la suite.

En matière de données, nous sommes présentement dans le far west. Cela va tellement vite. Les entreprises comme Google et Facebook peuvent obtenir des renseignements personnels sur les gens. Après, c'est le vide. On peut faire n'importe quoi parce qu'on a les données, qui ont été données par les gens de façon consentante.

En ce qui concerne ces instruments, la stratégie de Google est de vendre des services et de donner des services à la population. Comment allez-vous sécuriser les données que vous pouvez conserver? Pouvez-vous utiliser ce genre de robot pour aller chercher des données que vous allez revendre à d'autres plus tard?

● (1020)

[*Traduction*]

M. Colin McKay: Je vais commencer par répondre à votre dernière observation, c'est-à-dire que nous ne revendons pas l'information, alors ce n'est pas un facteur.

Pour ce qui est de Google Duplex, le projet dont il a été question à notre conférence de concepteurs cette semaine, c'est un projet. Il n'a pas encore été mis en oeuvre. C'est une tentative pour trouver comment offrir un service. À l'heure actuelle, vous pouvez parler à votre téléphone et demander le numéro de téléphone d'un restaurant, puis composer le numéro du restaurant et essayer de fixer un rendez-vous. Nous essayons de voir comment utiliser l'intelligence artificielle pour réaliser tout le processus de prise de réservation à votre place.

La portée de ce projet est très limitée. Je pense que trois ou quatre exemples ont été donnés lors de la conférence. Ce sont là les trois ou quatre choses qu'il peut faire. Il vise à fournir un service à la personne. Il ne s'agit pas de recueillir de l'information. Il s'agit d'un complément à la relation que nous entretenons avec un utilisateur de Google, qui a trait à l'information qu'il cherche, à sa façon d'inscrire l'information dans son calendrier et à sa façon de trouver des endroits où manger sur Google Maps.

Pour ce qui est de votre question sur les enquêtes plus vastes, ce n'est même pas envisagé à l'heure actuelle. Pour l'instant, nous ne menons pas de sondages d'envergure qui suscitent l'intérêt des électeurs ou des utilisateurs, alors il ne s'agit pas de mettre en oeuvre ce genre d'outil.

Je dois souligner qu'il s'agit d'utiliser l'intelligence artificielle de façon à accomplir des tâches banales de façon à ce que l'utilisateur en bénéficie, qu'elle lui fasse gagner du temps et qu'elle rende l'interaction aussi efficace que possible, tout en offrant un service clair à l'utilisateur.

[*Français*]

M. Jacques Gourde: Monsieur Balsillie, parlons de l'ensemble des données recueillies par les grands de ce monde, qui ont accès directement ou indirectement à notre vie privée. Si j'utilise mon assistant virtuel pour faire une réservation au restaurant. Au bout d'un an, Google va savoir que je vais chez Saint-Hubert une fois toutes les deux semaines, par exemple. Cela se multiplie. Il va savoir où est mon garage préféré et quelle est ma marque d'auto. Il s'agit d'une foule de données qui peuvent être réutilisées. Or je les ai transmises de façon volontaire en choisissant un restaurant.

Vous avez dit qu'il fallait encadrer et légiférer l'utilisation des données personnelles, mais si ces dernières sont transmises de façon volontaire, que peut-on faire? Si je donne mon numéro de téléphone personnel à mes amis, c'est parce que je veux qu'ils m'appellent. Lors de poursuites judiciaires, les géants du Web diront que les données qu'ils ont reçues leur ont été transmises de façon volontaire. Par exemple, des gens peuvent publier une photo d'eux sur Facebook où ils ont les cheveux rouges parce qu'ils aiment se teindre les cheveux en rouge. On ne peut rien faire contre cela.

Qu'en pensez-vous?

[*Traduction*]

Me Jim Balsillie: Je vous remercie pour ces questions.

Comprenons bien une chose: des volumes énormes de données sont recueillis sans transparence, sans que nous le sachions. Le RGPD a révélé que les plateformes des médias sociaux détiennent des millions de pages d'information sur chacun de nous sans que nous le sachions. On y retrouve toutes les activités que vous avez menées dans Internet pendant l'année.

Ces grandes sociétés réunissent de nombreuses autres choses, différents ensembles de données; elles font ce qu'on appelle du « hachage ». Il s'agit d'énormes ensembles de données que vous n'avez pas consenti à distribuer. Je vous dirai que les questions que vous me posez m'encouragent, parce que je vois ainsi que vous ne vous laisserez pas berner par de belles expressions vides de sens comme « consentement éclairé », « transparence » ou « nuance ». Ce sont des attrape-nigauds. Faites très attention quand on vous dit qu'on ne revendra pas vos renseignements, parce que... Peut-on exploiter des renseignements? Il faut que vous compreniez que des volumes énormes de renseignements sont recueillis sans que vous le sachiez.

Avez-vous entendu parler de Sidewalk Labs? Comment empêcher cette société de recueillir tous ces renseignements sur vous? Un reportage est sorti récemment sur la façon dont des employés de Facebook collaboraient avec des hôpitaux pour anonymiser les renseignements personnels sur la santé puis, en effectuant des renvois par intelligence artificielle dans les médias sociaux personnels des patients, ils réussissaient à extraire leur identité.

Il faut donc faire très attention à ces allégations de consentement éclairé et de volontarisme au sein d'un État de surveillance. Comme nous l'avons dit plus tôt, ces façons de faire progressent tellement rapidement que nous n'avons pas le temps de les comprendre, et nous glissons à toute vitesse vers un État de surveillance. Comme ce portrait que je vous dépeins vous l'indique, cela touche tous les aspects de notre citoyenneté souveraine et cela s'étend bien au-delà de l'économie.

● (1025)

[*Français*]

M. Jacques Gourde: Sera-t-il possible, dans les années à venir, d'avoir une vie privée, une intimité, alors que toutes ces données sont recueillies?

Dans cinq ou dix ans, sera-t-il encore possible d'avoir une vie privée?

[*Traduction*]

Me Jim Balsillie: Oui, mais il faudra pour cela établir des règles et des règlements responsables pour la société. Les Européens en ont débattu de ce problème pendant près de 10 ans. Ils ont découvert les moyens de nuancer leur position. Le RGPD européen n'a rien d'extrême. Les Européens ont trouvé le moyen d'établir une société ouverte et novatrice tout en protégeant la transparence et la vie privée de leurs citoyens. C'est tout à fait réalisable, mais il faut une réglementation responsable, experte et technique. Il a fallu neuf ans à l'Europe pour y parvenir.

Le président: Merci, monsieur Gourde.

Monsieur Angus, vous avez maintenant sept minutes.

M. Charlie Angus: Merci beaucoup.

Monsieur McKay, je suis heureux de vous avoir ici, et vous aussi, monsieur Balsillie.

Monsieur McKay, vous nous avez dit que votre entreprise est profondément enracinée au Canada. Dans ma région, vous faites une telle concurrence à tous les journaux locaux qu'ils ont de la peine à placer leur publicité en ligne. Pourriez-vous ancrer vos racines plus en profondeur en payant la taxe harmonisée afin d'équilibrer les règles du jeu?

M. Colin McKay: Je vous répondrai en deux étapes. D'abord, nous fournissons des services de technologie publicitaire aux journaux et nous fournissons des revenus...

M. Charlie Angus: Oui, mais cela ne m'intéresse pas. Dites-moi une chose: désirez-vous payer de l'impôt?

M. Colin McKay: Ne confondons pas les choses. Votre étude se fonde sur le comportement d'une seule entreprise. Nous fournissons des services aux journaux afin d'augmenter les revenus qu'ils tirent de leurs abonnés en ligne.

Pour répondre à votre deuxième question au sujet de la TPS, ma réponse est oui. Si le gouvernement prend les mesures nécessaires pour que la TPS s'applique à notre entreprise et aux autres entreprises qui font affaire en ligne, alors nous prendrons les mesures nécessaires, comme nous le faisons dans les autres pays, pour recueillir la TPS des utilisateurs qui achètent nos produits.

M. Charlie Angus: Est-ce que la ministre Joly se dirige dans cette voie?

M. Colin McKay: Je ne pense pas que cela relève de la ministre Joly, n'est-ce pas? Cela dépendrait plutôt du ministre Morneau. C'est au gouvernement d'en décider.

M. Charlie Angus: Nous entendons dire que votre société ne paie pas la TVH, mais elle n'est pas non plus visée par l'article 19 de la Loi de l'impôt sur le revenu; alors si vous ne payez pas la TVH en tant qu'entreprise canadienne, pourquoi les autres entreprises devraient-elles obtenir une déduction fiscale pour vous confier leur publicité? Google a qualifié de punitive l'obligation de payer des impôts sur ces annonces publicitaires. Nous dites-vous maintenant que ce n'est pas punitif, que ce serait équitable?

M. Colin McKay: Tout d'abord, nous payons des impôts sur certaines de nos ventes, comme les appareils et d'autres éléments de nos ventes au Canada.

M. Charlie Angus: Oui, en effet. Vous êtes obligés de le faire.

M. Colin McKay: Je vous dis simplement que si le gouvernement édicte une loi pour nous obliger, nous et les autres entreprises en ligne, de recueillir la TVH en son nom, nous prendrons les mesures nécessaires pour le faire.

M. Charlie Angus: Parfait.

J'ai remarqué qu'en 2014 au Royaume-Uni, Google a payé moins de 7 000 $ en impôt, ce qui représente à peu près la moyenne de ce que paient les travailleurs dans ce pays, et pourtant vous avez versé 534 millions de dollars en primes. Les règles du jeu équitables qui vous favorisent partout au monde vous conviennent très bien.

J'aimerais aborder la question de la philosophie de Google. J'étais un grand adepte de Google. Lorsque vous avez commencé, j'ai trouvé cela vraiment génial. J'ai visité Google à New York. J'ai adoré sa philosophie, de ne rien faire de malfaisant. Malheureusement, votre fondateur a aussi dit que la politique de Google dans bien des situations consiste à avancer jusqu'à la limite du dégoûtant sans toutefois la franchir.

Saurez-vous distinguer le dégoûtant acceptable du dégoûtant excessif et de ce qui est carrément malfaisant, quand vous ferez face à un recours collectif pour avoir recueilli illégalement des données? En utilisant une échappatoire sur iPhone, vous avez suivi des citoyens en temps réel sans leur consentement. Vous faites face à des accusations dans plusieurs États. Il y a maintenant une plainte de collecte de renseignements personnels sur des enfants de moins de 13 ans sans le consentement de leurs parents; vous les avez localisés, vous avez identifié leurs appareils et leurs numéros de téléphone et vous avez suivi leur utilisation de différents sites Web. Plutôt que de nous fier à vous pour déterminer ce qui est dégoûtant, ne devrions-nous pas simplement édicter une loi?

● (1030)

M. Colin McKay: Voilà pourquoi, dans mon allocution, je vous ai présenté une série d'outils que nous avons développés pour les utilisateurs. Vous avez raison. Il faut que nous indiquions avec transparence les renseignements que nous recueillons et que nous expliquions clairement pour quelles raisons nous le faisons et quels avantages les utilisateurs en retirent. Au fil des ans, nous avons tiré des leçons de nos erreurs. Nous avons beaucoup appris d'incidents comme ceux que vous décrivez ici.

M. Charlie Angus: Ce ne sont pas des erreurs. Ce sont des recours collectifs devant les tribunaux. Ce sont des accusations. Si vous vous faites prendre et que vous en tirez des leçons, vous vous trouvez dans la même situation que Facebook. Si votre politique publique est d'aller jusqu'à la dernière limite du dégoûtant, vous ne me réconfortez pas vraiment.

M. Colin McKay: Notre politique publique ne consiste pas à mettre nos utilisateurs mal à l'aise. Nous visons à développer des produits de fine pointe qui procurent la plus vaste gamme possible d'avantages à nos utilisateurs. Les gens les adoptent à des rythmes différents avec différents degrés d'aise.

M. Charlie Angus: Merci.

Monsieur Balsillie, ce que vous nous avez dit au sujet du capitalisme de surveillance m'intéresse beaucoup. Je ne voulais absolument pas que l'on réglemente Google parce que je voulais le laisser évoluer. Imaginez, moi un socialiste, me voici face à un entrepreneur qui nous met en garde contre le capitalisme de surveillance. C'est le monde à l'envers.

Je suis vraiment inquiet du fait qu'au Canada, l'ancien directeur des politiques de Google se trouve au bureau de la ministre du Patrimoine canadien. Aux États-Unis, le directeur des brevets de Google est maintenant au bureau des brevets. On craint beaucoup que l'énorme pouvoir de Google n'affaiblisse la loi américaine sur les brevets. La Banque du Canada nous a mis en garde contre le pouvoir d'entreprises comme Google qui risque de miner la compétitivité. Dans le secteur de la technologie, l'avocat spécialiste des brevets, Michael Shore, a dit que les États-Unis se transforment en une « république de bananes », parce que les législateurs réécrivent la loi pour protéger les intérêts de géants comme Google. Entre-temps, les États-Unis sont passés du premier au 12e rang du classement mondial des brevets au cours de ces quatre dernières années.

Quant au secteur canadien de la technologie, vu la relation extrêmement amicale que le gouvernement actuel entretient avec Google, dans quelle voie se dirige notre secteur de la technologie sur le plan de l'innovation? Réussira-t-il à gagner la confiance des consommateurs canadiens dans le domaine de la protection de la vie privée?

Me Jim Balsillie: Je m'inquiète profondément du fait que ces partenariats ont été conclus sans que l'on ait mené une analyse économique au pays. Franchement, je ne sais pas quoi vous répondre. Je sais que dans le monde des affaires, ils ont des effets indirects très négatifs sur nos résultats en matière d'innovation. Vous voyez que cette année, le Canada a pris du retard sur la Pologne sur le plan de l'innovation. Nous sommes donc au 22e rang dans le monde alors que la Pologne est maintenant 21e. Quand une nation ne fait plus partie des 20 premières, elle n'est plus vraiment considérée comme une nation novatrice. J'établirais un lien direct entre ce rendement et le fait que nous n'ayons pas créé d'approches de diffusion souveraines positives en matière d'innovation.

Pour répondre à votre question, je pense que nous nous hâtons trop. Je sais pertinemment que ces partenariats n'ont pas fait l'objet d'analyses économiques et que l'on n'a pas demandé les conseils d'experts sur les résultats attendus. Il est inimaginable qu'une entreprise établisse un partenariat sans mener une analyse de rentabilisation. La première chose à faire serait d'analyser les effets novateurs de ces divers partenariats, ou de ces relations, en se fondant sur de bons principes économiques et non sur des principes que j'appellerais « lobbynomiques ».

Deuxièmement, comme je l'ai dit en parlant de l'Estonie et de l'Union européenne, qui suit des stratégies très actives en matière de concurrence, la Loi sur la concurrence et la Loi sur la protection des renseignements personnels ont la capacité de fortement favoriser l'innovation, l'économie et la citoyenneté. Ensemble, ces lois créent d'excellents avantages dans ces domaines si l'on y applique bien leur véritable nature.

M. Charlie Angus: Merci.

Le président: Merci, monsieur Angus.

Je viens de parler à Jean-Denis. Nous allons poursuivre cette séance jusqu'à presque 11 heures. Une autre réunion va commencer ici à 11 heures.

Alors sans plus tarder, nous passons la parole à M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Monsieur Balsillie, vous avez indiqué dans votre déclaration préliminaire que vous classiez Facebook et Google avec les entreprises de mégadonnées. De toute évidence, Facebook et Cambridge Analytica ont suscité cette étude, et je voyais bien qu'en partageant un tel volume d'information avec des développeurs tiers d'applications, comme Facebook l'avait fait, ces sociétés enfreignaient notre loi. En fait, leurs représentants ont comparu devant nous pour nous dire qu'ils n'étaient pas d'accord avec cette affirmation. Ils ont cependant ajouté que ces façons de faire n'étaient pas convenables et qu'ils avaient modifié leurs pratiques.

Monsieur Balsillie, vous avez mentionné Google et Facebook dans une même phrase. Voyez-vous à l'heure actuelle des pratiques de Google qui, selon vous, devraient changer, et si tel est le cas, pour quelles raisons?

● (1035)

Me Jim Balsillie: Je vois de nombreuses pratiques qui devraient changer.

Examinons d'abord l'éthique des algorithmes et la façon dont ils influent sur le comportement des gens. Vous avez parlé de publicité. On a beaucoup débattu des façons dont les algorithmes favorisent certains types de dissidence dans YouTube, par exemple, parce qu'ils sont conçus pour vous amener à regarder davantage de vidéos, et plus vous regardez ces vidéos, plus elles vous poussent vers des jugements extrêmes.

À mon avis, il faut réglementer adéquatement ces vidéos. Il faut y appliquer des normes adéquates. Nous avons constaté que les entreprises réagissent après s'être fait prendre, ce qui prouve la nécessité d'établir des règlements adéquats et responsables.

À mon avis, cette situation ressemble à celle où la Californie se préparait à légiférer sur les émissions des voitures. À ce moment-là, tout le monde s'est exclamé que ces lois causeraient l'effondrement de l'industrie automobile, qu'il serait impossible de l'innover et que cette initiative ne serait pas rentable. Nous avons maintenant de meilleures voitures, moins d'émissions, et les fabricants d'automobiles génèrent des profits records. Judicieusement appliquées, ces mesures se renforceront mutuellement. Je constate ici une voie sociale et capitaliste très positive à poursuivre.

M. Nathaniel Erskine-Smith: Monsieur McKay, j'ai ouvert les paramètres de Google Ads. Il semblerait que j'aime 59 éléments. Certains d'entre eux me plaisent vraiment, mais je ne suis pas adepte de la course et de la marche. J'aime cependant les films d'action. Cela dit, on ne me cible pas nécessairement en fonction de ces 59 éléments. Vous savez également où je suis allé avec ce cellulaire depuis 12 mois, si j'ai bien compris.

Je voudrais savoir dans quelle mesure vous soutirez des mots de mes Hangouts et de mes courriels. Vous êtes au courant de toutes les recherches que j'ai effectuées dans Google et vous avez examiné tous les sites Web que j'ai visités par Chrome et que j'ai inscrits dans mes signets, et plus encore. La publicité que je reçois ne porte pas sur ces 59 éléments. Pourquoi est-ce que l'on ne m'informe pas mieux que cela? Pourquoi y a-t-il si peu de transparence sur ces 59 éléments?

M. Colin McKay: Si vous faites une recherche plus approfondie dans cet outil, vous y trouverez l'historique des sites que vous avez consultés; vous avez consciemment accepté cela en configurant votre cellulaire. Vous pouvez en tout temps retourner à cet endroit et désactiver cet outil pour tous les services...

M. Nathaniel Erskine-Smith: Oui, je comprends, et je vous ai dit que je savais que vous étiez au courant des sites que j'ai visités au cours de ces 12 derniers mois.

Ma question porte sur la transparence de la publicité. Quand je reçois une publicité, je n'ai pas moyen d'aller voir lesquels de mes renseignements ont servi à choisir cette annonce pour qu'on l'affiche à mon écran de consommateur. Pourquoi?

M. Colin McKay: Si vous fouillez un peu dans certaines sections de notre réseau publicitaire, vous y trouverez un petit D affiché à l'envers. Vous pressez dessus, et vous verrez pourquoi cette annonce se trouve dans notre réseau d'affichage publicitaire.

M. Nathaniel Erskine-Smith: Je comprends. Facebook offrait aussi cette fonction, et je crois qu'elle s'y trouve encore. Il va falloir l'améliorer, et vous devrez peut-être aussi le faire, parce qu'on nous explique simplement que nous avons apprécié des choses similaires dans Internet.

M. Colin McKay: Oui.

M. Nathaniel Erskine-Smith: Ce n'est pas du tout un niveau de transparence acceptable. À quel point votre transparence est-elle détaillée?

M. Colin McKay: Eh bien, vous venez de nous la décrire. Vous avez ouvert cette fonction pendant que nous parlions, et vous y avez trouvé 59 éléments, dont certains sont erronés. Je dois vous dire que pendant plusieurs années, la majorité des employés de Google pensaient que j'étais une femme.

M. Nathaniel Erskine-Smith: Vous ne vous basez pas seulement sur ces 59 éléments, n'est-ce pas? Ce n'est pas possible. Vous utilisez tout ce que j'ai cherché dans Google, vous utilisez mon historique de navigateur. Il ne s'agit pas seulement de ces 59 éléments. Quand je reçois une annonce, je ne peux pas en faire tout le suivi. Je ne peux pas connaître toutes les raisons pour lesquelles j'ai été ciblé, si je l'ai été parce que j'avais fait une recherche dans un site Web ou que j'ai cherché quelque chose le 1er mai. Je ne peux pas savoir ces choses, n'est-ce pas?

M. Colin McKay: Nous visons des objectifs semblables vous et moi, et vous avez raison. Vous devriez être en mesure de comprendre comment vous nous fournissez vos renseignements et comment nous les utilisons pour fournir des services. Nous essayons de le faire dans une suite que nous avons mise au point, que ce soit par l'entremise de Mon compte ou de la fonction Confidentialité et sécurité. De toute évidence, vous me signalez une situation où vous n'obtenez pas toute l'information qui vous rassure.

M. Nathaniel Erskine-Smith: Oui, parce que ce qui m'inquiète, c'est que Rob Sherman nous a dit qu'en effet, ils n'avaient pas fait ce qu'ils auraient dû à l'époque. Dans trois ans, allez-vous revenir témoigner en nous disant qu'en effet, vous n'auriez pas dû faire ce que vous faites maintenant? Nous devons réglementer, mais si vous croyez vraiment à l'importance de la transparence, vous devriez dès maintenant agir avec plus de transparence que vous ne le faites.

En ce qui concerne les courriels et les Hangouts, si j'envoie un courriel à des amis pour leur présenter mes condoléances et pour leur promettre d'aller aux funérailles, ou si j'écris à une amie que je suis heureux d'apprendre qu'elle vient de donner naissance à son enfant, est-ce que ces amis vont commencer à recevoir des annonces sur des services funéraires ou sur des poussettes?

M. Colin McKay: S'ils utilisent nos produits, non. Nous n'envoyons pas d'annonces en fonction du contenu de vos courriels ou de vos Hangouts. Nous effectuons des recherches dans votre contenu pour veiller à ce que vous ne receviez pas de maliciels, de tentatives d'hameçonnage ou d'atteinte à votre sécurité personnelle. Nous utilisons des systèmes automatisés pour assurer la sécurité de votre compte, mais nous ne diffusons pas d'annonces en fonction du contenu de vos courriels de Gmail. Surtout dans les deux contextes que vous venez de décrire...

● (1040)

M. Nathaniel Erskine-Smith: Dites-moi de quelles autres manières vous ciblez les annonces publicitaires à partir de l'historique de mes courriels ou de mes Hangouts.

M. Colin McKay: Eh bien, les Hangouts ne vous enverraient pas de publicité. Par Gmail, vous recevez des annonces générales en fonction du genre de personne que nous pensons que vous êtes. Nous ne les ciblons pas à partir du contenu de votre boîte de réception ou de vos courriels, pas du tout.

M. Nathaniel Erskine-Smith: Bon, d'accord.

Ma dernière question porte sur les applications développées par des tiers. Certains développeurs d'applications de la plateforme de Facebook nous ont dit qu'ils recevaient une multitude de renseignements qui n'avaient aucun lien avec l'application qu'ils devaient livrer et qui dépassaient largement la portée de ce dont ils avaient besoin pour la créer.

Expliquez-moi en détails comment vous partagez vos applications développées par des tiers et quels renseignements vous fournissez à ces développeurs.

M. Colin McKay: Bien sûr. Nous ne fournissons aucuns renseignements aux développeurs tiers...

M. Nathaniel Erskine-Smith: Non, mais vous leur donnez accès aux renseignements de base sur les comptes...

M. Colin McKay: Oui, les renseignements de base sur les comptes, comme les adresses courriel...

M. Nathaniel Erskine-Smith: Quels sont les renseignements de base sur mon compte?

M. Colin McKay: L'adresse courriel et le nom. Il s'y trouve un troisième renseignement, mais il n'est pas confidentiel. Les développeurs d'applications tiers reçoivent ces deux renseignements, puis nous négocions avec eux pour qu'ils nous fournissent...

M. Nathaniel Erskine-Smith: Donc aucun développeur d'applications tiers ne recevrait d'autres renseignements que cette information de base sur le compte?

M. Colin McKay: Aucun développeur d'applications tiers ne pourra donc avoir accès à d'autres renseignements, dans certaines circonstances, sans en avoir discuté avec vous et sans avoir demandé et avoir obtenu votre consentement à ce que le développeur d'applications fournisse l'information...

M. Nathaniel Erskine-Smith: Mais, c'est clair, n'est-ce pas? C'est comme... Je ne sais peut-être pas ce que j'accepte, toute l'information n'étant pas divulguée en particulier aux consommateurs moyens pour leur dire qu'ils acceptent *xy* et *z* et beaucoup d'information sera diffusée.

M. Colin McKay: Lorsque vous installez une application sur un téléphone Android sous licence, on vous donne un menu précis qui doit comporter un lien vers une politique de confidentialité complète et claire afin que vous compreniez la position de la compagnie à l'égard de la protection de la vie privée et de la sécurité. Puis, les renseignements qui sont conservés ou générés par le téléphone ou par votre compte et auxquels elle demande accès sont spécifiquement indiqués. Sur une application de Google Play pour un téléphone Android, vous devez être capable de vous connecter et de voir plus en détail pourquoi la compagnie veut cette information.

Le président: Merci, monsieur Erskine-Smith. J'aimerais vous accorder plus de temps.

C'est maintenant au tour de M. McCauley, pour cinq minutes.

M. Kelly McCauley: Merci monsieur Erskine-Smith pour ces renseignements très intéressants.

Monsieur Balsillie, vous avez parlé du RGPD de l'Union européenne. Y a-t-il quelque chose que vous changeriez si le Canada adoptait quelque chose de semblable?

Me Jim Balsillie: Selon les principes de base, non. Les aspects sur lesquels je m'attarde sont, premièrement, que vous êtes propriétaires de vos données et que vous les contrôlez, que vous êtes au courant de ce que les intervenants font et que vous avez ce qu'on appelle le droit de supprimer et le droit de transférabilité.

La deuxième chose, dont nous n'avons pas beaucoup discuté, qui est un élément très central du RGPD et qui a donné lieu à un énorme bras de fer entre Bruxelles et Washington pendant de nombreuses années, c'est cet élément de sécurité des itinéraires. Il importe de comprendre que, peu importe ce que nous réglementons au Canada, entre 80 et 90 % de nos données passent par les États-Unis, selon ce que m'ont dit des experts. Même si je vous envoie un courriel de l'autre côté de la table, il sera acheminé à l'extérieur. C'est ce qu'on appelle l'effet boomerang. Il faut comprendre que, selon la loi américaine, les données canadiennes n'ont aucun droit aux États-Unis. Vous n'avez aucun droit à la vie privée; vous n'avez aucun droit à quoi que ce soit. L'Union européenne a également géré le routage de façon à ne jamais abandonner la compétence sur le traitement approprié de ces données.

Le RGPD est nuancé. Il a fait l'objet d'un débat pendant bien des années et il a pris en compte de nombreux points de vue. Nous devrions adopter au Canada une approche à tout le moins semblable à celle qui a conduit au RGPD puis envisager d'autres formes d'activités, par exemple, les possibilités de développement économique pour les industries primaires dont M. MacKay a parlées et bien d'autres aspects que nous pourrions étendre au-delà de cela.

Il est également très important de se rappeler, même si ce n'est pas du ressort du Comité, qu'en parallèle, l'UE a fait un ensemble soutenu d'études et de plans sur le comportement de la concurrence pour ce qu'on appelle l'asymétrie inhérente des données, où les gros deviennent plus gros. Si vous voulez promouvoir le progrès économique et la prospérité, vous devez aussi tenir compte des structures concurrentielles.

La concurrence et le RGPD ont progressé en harmonie pendant les travaux qui ont duré une bonne dizaine d'années.

M. Kelly McCauley: C'était ma question complémentaire. Vous avez parlé de la valeur des données. Ma question était la suivante: comment pouvons-nous monétiser cela au Canada tout en protégeant la vie privée? Cependant, je vais passer à la question suivante: quel est le rôle des monstres Facebook et Google au Canada dans le système où nous voulons monétiser la valeur pour les Canadiens et non seulement pour les grands qui deviennent plus grands?

● (1045)

Me Jim Balsillie: Je ne les vois pas comme des monstres. Je les vois seulement comme des capitalistes.

M. Kelly McCauley: Désolé, les géants.

Me Jim Balsillie: Ce sont des capitalistes et le travail d'une société est de faire ce qu'une société est censée faire et le travail du gouvernement est de réglementer. C'est une question complexe parce que c'est la plus grande force de l'histoire du capitalisme qui permet, par exemple, à six entreprises venues de nulle part de devenir les plus précieuses au monde en très peu de temps. Il est très important de savoir comment les structures concurrentielles et réglementées sont gérées et comment nous pouvons le faire dans l'intérêt de l'économie canadienne et des innovateurs canadiens. Des éléments comme le comportement concurrentiel et la propriété des données doivent également être pris en compte dans une stratégie nationale de gestion des données qui tient compte de la prospérité et de bien d'autres facteurs connexes, comme les règles en matière d'emploi, les règles cybernétiques, etc. C'est un gros dossier, et nous devons le traiter de toute urgence de façon horizontale à titre de nation et de décideurs.

M. Kelly McCauley: Nous, au gouvernement, ne sommes pas les plus rapides. Si nous devions aborder la question du RGPD, cela pourrait prendre des années.

Les choses bougent tellement vite. Sur quoi devrions-nous porter notre attention, pour ajuster le tir en cours de route, afin de ne pas adopter un RGPD s'appuyant sur des règles et sur la réalité d'hier?

Me Jim Balsillie: À mon avis, il faut tenir compte du fait que cela fait neuf ans que les responsables y travaillent en Europe et que nous nous y attaquons maintenant. Ce n'était pas nécessaire dans ce pays. Je pense que nous devons réfléchir à la nécessité d'être à jour et de faire appel à des experts.

Je pense que vous avez entendu d'excellents témoignages de gens comme le commissaire Therrien sur la mise à jour de nos règles en matière de protection de la vie privée. Je crois que le Bureau de la concurrence est venu vous parler des pratiques de concurrence mises à jour.

Il y a eu pas mal de travail de fait. J'encourage nos législateurs à se rallier à cette idée et à dire que 2018 est l'année de la réglementation et de la législation du capitalisme de la surveillance des données et de l'économie axée sur les données au profit des citoyens canadiens, maintenant et à long terme.

Le président: Merci, monsieur McCauley.

C'est maintenant au tour de M. Baylis, pour cinq minutes.

M. Frank Baylis: Merci, monsieur le président.

En ce qui concerne les règles du RGPD, je suis d'accord avec M. Balsillie.

Diriez-vous que ce sont les règles les plus rigoureuses au monde à l'heure actuelle et que nous devrions envisager de les adopter?

Me Jim Balsillie: Elles fixent la norme, oui.

M. Frank Baylis: Elles fixent la norme.

Monsieur McKay, lorsque les règles du RGPD sont entrées en vigueur, Facebook a délibérément transféré une bonne partie de ses données de l'Irlande à l'extérieur du territoire où sont appliquées les règles.

Google a-t-elle pris de telles mesures?

M. Colin McKay: Non.

M. Frank Baylis: Vous devez maintenant envisager de vous conformer à ces règles du RGPD. Quelles mesures prenez-vous pour vous y conformer, si vous n'avez pas pris de mesures pour vous en éloigner?

M. Colin McKay: Nous investissons dans les équipes et nous améliorons nos outils pour nous conformer au RGPD depuis très longtemps. C'est un défi extrêmement complexe, même pour une entreprise de notre taille. C'est un défi encore plus grand, non seulement pour les petites entreprises, mais aussi pour les commissaires à la protection de la vie privée en Europe.

Ce que nous faisons se reflète dans les outils que j'ai mentionnés dans ma déclaration préliminaire. Cela se reflète dans le genre de permissions et de contrôle que chaque utilisateur a sur tous nos services partout dans le monde.

Les obligations imposées par le RGPD et les attentes concernant la protection des données en Europe trouvent écho dans les services fournis par Google aux utilisateurs du monde entier.

M. Frank Baylis: Les utilisateurs du monde entier vont donc bénéficier du RGPD. N'allez-vous pas avoir un système à deux vitesses?

M. Colin McKay: Partout dans le monde, les utilisateurs tirent profit de l'attention accrue accordée à la confiance, à la transparence et au contrôle individuel. C'est le point de départ du RGPD et des autres régimes de protection des données.

M. Frank Baylis: Soyons précis. M. Balsillie nous dit que ces règles sont ce qui se fait de mieux dans le moment.

Vous ne ménagez pas vos efforts pour vous conformer à ces règles. Vous n'avez pas transféré vos données, comme Facebook l'a fait, pour les contourner. Ces règles seront établies. Vous avez programmé pour l'Europe. Est-ce que tout le monde partout sans exception va tirer profit de ces règles ou devons-nous, comme l'a suggéré M. Balsillie, établir nos propres règles et retourner voir Google pour lui dire qu'il vaut mieux adhérer à la version canadienne du RGPD?

M. Colin McKay: Je pense que si on envisage ce qui se fait de mieux dans la catégorie, qui aide tout le monde et qui normalise les obligations en matière de protection des données, alors pour le moment, c'est le RGPD qui remporte la palme. Il est le moteur du changement dans notre entreprise et dans d'autres.

De même, il pose un enjeu de taille aux entreprises dont les systèmes internes de TI ne sont pas perfectionnés ou qui ne comprennent pas bien les données qu'elles détiennent et les responsabilités qui leur incombent envers les utilisateurs, en particulier les entreprises qui essaient d'exporter en Europe ou d'importer d'Europe ou qui ont des liens avec des clients en Europe. Au cours des six prochains mois, à tout le moins, les entreprises s'efforceront de comprendre les obligations qui leur incombent aux termes du RGPD.

● (1050)

M. Frank Baylis: Si elles n'ont pas la taille de votre entreprise, elles devront probablement simplement s'y conformer et dire que tout ce qu'elles font est conforme au RGPD.

M. Colin McKay: Non, le défi pour elles consiste en fait...

M. Frank Baylis: Je vous demande si Google va le faire.

M. Colin McKay: Oui.

M. Frank Baylis: Est-ce que Google va s'assurer que si une personne effectue une transaction au Japon ou parle du Canada ou du Japon, peu importe, les règles mises en place pour respecter le RGPD vont protéger toutes les autres activités qui ne touchent pas vraiment l'Europe ou qui ne passent pas par l'Europe?

M. Colin McKay: Il y aura des améliorations de suivi et un contrôle accru de la transparence du fait de notre conformité au RGPD.

M. Frank Baylis: Les utilisateurs auront-ils droit au même traitement? Je suis persuadé qu'ils s'amélioreront, mais obtiendront-ils la même chose que le RGPD ou allez-vous intentionnellement faire un triage et traiter celui-ci aux termes du RGPD et celui-là, non?

M. Colin McKay: Nous n'allons pas faire de choix explicites comme celui-là. Ce que nous faisons, comme cela a été mentionné dans la conversation, c'est... Les lois sur la protection des données et la protection des renseignements personnels varient d'un pays à l'autre. Nous devons respecter les obligations de chaque pays. Ce que les utilisateurs vont constater, c'est que l'ensemble des contrôles et des outils à leur disposition s'améliorent grâce à la fois à notre investissement et aux obligations découlant du RGPD.

M. Frank Baylis: Y a-t-il eu des atteintes à la sécurité des données dans les bases de données de Google comparativement à ce qui s'est passé avec Facebook?

M. Colin McKay: D'après ce que nous savons, non.

M. Frank Baylis: D'accord.

Vous avez dit que vous ne vendiez pas les données. Je suis d'accord avec vous. Pourquoi les vendre? Elles vous appartiennent. C'est tout à fait valable. Vous n'avez qu'à les louer et laisser les gens vous les demander. C'est votre modèle. Est-ce exact?

M. Colin McKay: Nous possédons les données que nous avons à votre sujet et nous les utilisons pour vendre de la publicité.

M. Frank Baylis: La personne qui a volé les données de Facebook s'est demandé pourquoi elle donnerait des données qu'elle pourrait utiliser pour vendre de la publicité même aux mauvais acteurs. Il fallait que quelqu'un s'immisce, simule et vole.

Est-ce que quelqu'un a essayé? Est-ce que cela arrive à Google?

M. Colin McKay: Pas d'après ce que nous avons vu.

Le président: Merci, monsieur Baylis. Nous arrivons pile à la fin de la séance.

Merci à tout le monde...

Monsieur Angus.

M. Charlie Angus: Monsieur le président, comme nous avons été un peu pressés au cours de ce tour en raison du dernier tour et que nos deux témoins nous ont fourni énormément d'information, je me demande s'il est possible de leur envoyer des questions. Nous n'avons pas abordé des aspects comme la ville intelligente, la modération de Google Maps et certaines questions sur l'innovation.

Je me demande simplement s'il serait possible, par l'entremise du président, de poser des questions pour que nous puissions nous assurer d'avoir fait preuve de toute la diligence voulue.

Le président: Absolument.

Êtes-vous d'accord pour répondre à ces questions lorsqu'elles seront posées?

M. Colin McKay: Je suppose qu'elles seront acheminées par l'entremise du Comité.

Le président: Oui.

J'ai une seule question pour M. Balsillie et je suis désolé, mais votre temps est bel et bien écoulé.

Vous avez parlé de « capitalisme de surveillance ». Je suppose que la raison pour laquelle nous sommes ici aujourd'hui, c'est qu'il y a un risque de fraude électorale quelque part dans un autre pays. Si nous ne modifions pas nos lois au Canada pour faire face au capitalisme de surveillance, notre démocratie est-elle menacée?

Me Jim Balsillie: Sans aucun doute.

Le président: Merci.

Merci à tous d'être venus aujourd'hui.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur.* Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur.*

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes
à l'adresse suivante : http://www.noscommunes.ca

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act.* Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act.*

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the
following address: http://www.ourcommons.ca